(19)日本国特許庁（ＪＰ）　(12) **公開特許公報**（Ａ）　(11)特許出願公開番号

特開平10－173646

(43)公開日　平成10年(1998)６月26日

(51)Int.Cl.[6]		識別記号	FI		
Ｈ０４Ｌ	9/34		Ｈ０４Ｌ	9/00	６８１
Ｇ０９Ｃ	1/00	６１０	Ｇ０９Ｃ	1/00	６１０Ａ
		６５０			６５０Ｚ
Ｈ０４Ｌ	9/14		Ｈ０４Ｌ	9/00	６４１

審査請求　未請求　請求項の数10　ＯＬ　（全９頁）

(21)出願番号　特願平8－334023

(22)出願日　平成８年(1996)12月13日

(71)出願人　000006013
三菱電機株式会社
東京都千代田区丸の内二丁目２番３号

(72)発明者　長谷川　俊夫
東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内

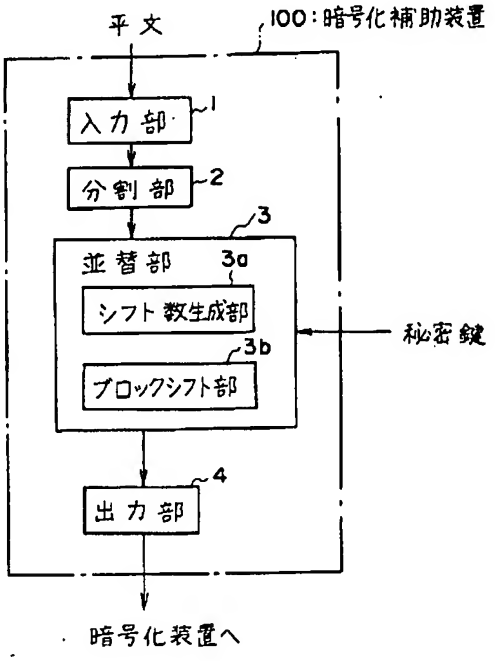
(74)代理人　弁理士　吉田　研二　（外２名）

(54)【発明の名称】　暗号化補助方法、復号化補助方法、およびそれらの方法を用いた装置

(57)【要約】

【課題】　暗号ブロック連鎖方式を用いて平文を暗号化しても、その第一文にはフィードバック効果がなく、暗号強度が低かった。

【解決手段】　暗号化補助装置は、暗号化すべき平文列を入力する入力部１、入力された平文列を所定長のブロックに分割する分割部２、暗号鍵の情報をもとに、分割されたブロックを並べ替える並替部３、並替後のブロックを先頭から順に後段の暗号化装置に出力する出力部４をもつ。秘密鍵のデータが例えば「３、１、２…」のとき、第一ブロックを右に３、第二ブロックを右に１、第三ブロックを右に２シフトし、ブロックの順序を入れ替える。



1

【特許請求の範囲】

【請求項１】　暗号化すべき平文列を所定長のブロックに分割し、暗号化に用いる暗号鍵の情報をもとにブロックを並べ替え、並替後のブロックを先頭から順に暗号化処理工程に引き渡すことを特徴とする暗号化補助方法。

【請求項２】　復号化処理工程で復号化された平文列を受け取り、復号化に用いた暗号鍵の情報をもとにその平文列を構成するブロックを並べ替え、並替後のブロックを先頭から順に出力することを特徴とする復号化補助方法。

【請求項３】　暗号鍵を用いた平文の暗号化に際して補助処理を行う装置であって、
暗号化すべき平文列を入力する入力手段と、
入力された平文列を所定長のブロックに分割する分割手段と、
暗号鍵の情報をもとに、分割されたブロックを並べ替える並替手段と、
並替後のブロックを先頭から順に暗号化処理部に出力する出力手段と、
を有することを特徴とする暗号化補助装置。

【請求項４】　暗号鍵を用いた暗号文の復号化に際して補助処理を行う装置であって、
復号化処理部で復号化された平文列を入力する入力手段と、
暗号鍵の情報をもとに、入力された平文列を構成する各ブロックを並べ替える並替手段と、
並替後のブロックを先頭から順に出力する出力手段と、
を有することを特徴とする復号化補助装置。

【請求項５】　所定の基準タイミングに関して時間変数を生成する時間変数生成手段をさらに含み、前記並替手段は暗号鍵の情報にこの時間変数を加味してブロックを並べ替える請求項３に記載の暗号化補助装置。

【請求項６】　暗号化の際の基準タイミングに関して生成された時間変数を取得する時間変数取得手段をさらに含み、前記並替手段は暗号鍵の情報にこの時間変数を加味してブロックを並べ替える請求項４に記載の復号化補助装置。

【請求項７】　ユーザーを識別するＩＤ情報を入力するＩＤ入力手段をさらに含み、前記並替手段は暗号鍵の情報にこのＩＤ情報を加味してブロックを並べ替える請求項３に記載の暗号化補助装置。

【請求項８】　暗号化の際に入力されたＩＤ情報を取得するＩＤ取得手段をさらに含み、前記並替手段は暗号鍵の情報にこの時間変数を加味してブロックを並べ替える請求項４に記載の復号化補助装置。

【請求項９】　乱数を生成する乱数生成手段をさらに含み、前記並替手段は暗号鍵の情報にこの乱数情報を加味してブロックを並べ替える請求項３に記載の暗号化補助装置。

【請求項１０】　暗号化の際に生成された乱数を取得する乱数取得手段をさらに含み、前記並替手段は暗号鍵の情報にこの乱数変数を加味してブロックを並べ替える請求項４に記載の復号化補助装置。

2

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、暗号化および復号化に際して補助的な処理を行う方法および装置に関する。

【０００２】

【従来の技術】従来の暗号方式として、米国の標準暗号である秘密鍵暗号方式ＤＥＳ（Data Encryption Standard）や素因数分解に着目する公開鍵暗号方式ＲＳＡ（Rivest－Shamir－Adlemen）が知られている。これらの暗号方式では、平文をある一定のブロックに区切り、ブロック単位で公開鍵または秘密鍵によって暗号化することにより、最終的に平文全体を暗号化することを特徴とする。これらの方式の暗号強度、すなわち解読のされにくさは非常に高いとされるが、処理をブロック単位で行うため、平文の種類などによってはブロックごとに一定の統計的性質を示す場合があり、これが暗号強度を低下させる原因になりうる。

【０００３】ブロックベースの暗号化強度を高めるために、暗号ブロック連鎖方式という方式が知られている。例えばＩＳＯ８３７２では、４種類の暗号モードＣＢＣ，ＯＦＢ，ＣＦＢ，ＥＣＢモードを規定している。これらのモード（ＥＣＢを除く）では、ひとつの平文ブロックを暗号化するたびに、その結果または経過に基づく情報を暗号器に回帰させ、その情報を次ブロック以降の暗号化に連鎖的に影響せしめる。これらのモードによれば、あるブロックの暗号化が過去の暗号化処理の履歴に依存するため解読が困難になる。

【０００４】こうした従来のブロックベースの暗号化装置として、図１０に実開昭５２－１３０５０５号公報に開示される装置の概念的な構成を示す。同図において、５０は、以前の出力データブロックであるデータワードに依存する数学的に可逆な関数と入力データブロックとを組み合わせる組合せ手段、５１は組合せ手段へデータワードを供給する供給手段、５２はユーザーの鍵をもとに暗号化を行う鍵制御方式暗号変換手段である。

【０００５】この構成にて、入力データブロックが入力されると、そのときすでに鍵制御方式暗号変換手段５２に存在していたデータワード５３が、供給手段５１によって組合せ手段５０へ出力される。組合せ手段５０は、データワード５３で決まる可逆関数と新規の入力データブロックを組み合わせ、その結果が鍵制御方式暗号変換手段５２へ渡される。鍵制御方式暗号変換手段５２は鍵の関数を適用してデータブロックを暗号化し、これを出力する。この出力は、新たなデータワード５３として供給手段５１へ渡される。

【０００６】

【発明が解決しようとする課題】暗号ブロック連鎖方式（ＣＢＣ、ＯＦＢ、ＣＦＢモードなど）では過去の暗号履歴を織り込んだ複雑な暗号化関数が用いられるため、解読は一般に困難になる。しかし、平文の第一ブロックを暗号化する際、そのブロックに先行するブロックが存在しないため、連鎖による効果は得られない。例えば電子メールを想定する場合、その文頭は定型であることが多く、この部分についてもとの平文データが予想されやすい。電子メールの内容が異なっていてもその第一ブロックは毎回同じ暗号化関数で処理されるため、同一のＣＢＣ方式の使用をつづけていくうちに解読の手がかりを与えてしまう可能性がある。

【０００７】本発明はこうした課題に鑑みてなされたものであり、その目的は、例えば第一ブロックなど、ブロックの位置に起因する暗号強度の低下を阻止する暗号化補助方法および装置を提供することにある。本発明の別の目的は、それらの方法または装置で暗号化された暗号文を平文に戻すことのできる復号化補助方法および装置を提供することにある。

【０００８】

【課題を解決するための手段】本発明の暗号化補助方法は、暗号化すべき平文列を所定長のブロックに分割し、暗号化に用いる暗号鍵の情報をもとにブロックを並べ替え、並替後のブロックを先頭から順に暗号化処理工程に引き渡すものである。

【０００９】一方、本発明の復号化補助方法は、復号化処理工程から復号化された平文列を受け取り、復号化に用いた暗号鍵の情報をもとにその平文列を構成するブロックを並べ替え、並替後のブロックを先頭から順に出力するものである。

【００１０】他方、本発明の暗号化補助装置は、暗号化すべき平文列を入力する入力手段と、入力された平文列を所定長のブロックに分割する分割手段と、暗号鍵の情報をもとに、分割されたブロックを並べ替える並替手段と、並替後のブロックを先頭から順に暗号化処理部に出力する出力手段とを有するものである。

【００１１】また、本発明の復号化補助装置は、復号化処理部で復号化された平文列を入力する入力手段と、暗号鍵の情報をもとに、入力された平文列を構成する各ブロックを並べ替える並替手段と、並替後のブロックを先頭から順に出力する出力手段とを有するものである。

【００１２】本発明の暗号化補助装置は、所定の基準タイミングに関して時間変数を生成する時間変数生成手段をさらに含み、前記並替手段は暗号鍵の情報にこの時間変数を加味してブロックを並べ替えるものである。

【００１３】本発明の復号化補助装置は、暗号化の際の基準タイミングに関して生成された時間変数を取得する時間変数取得手段をさらに含み、前記並替手段は暗号鍵の情報にこの時間変数を加味してブロックを並べ替えるものである。

【００１４】本発明の暗号化補助装置は、ユーザーを識別するＩＤ情報を入力するＩＤ入力手段をさらに含み、前記並替手段は暗号鍵の情報にこのＩＤ情報を加味してブロックを並べ替えるものである。

【００１５】本発明の復号化補助装置は、暗号化の際に入力されたＩＤ情報を取得するＩＤ取得手段をさらに含み、前記並替手段は暗号鍵の情報にこの時間変数を加味してブロックを並べ替えるものである。

【００１６】本発明の暗号化補助装置は、乱数を生成する乱数生成手段をさらに含み、前記並替手段は暗号鍵の情報にこの乱数情報を加味してブロックを並べ替えるものである。

【００１７】本発明の復号化補助装置は、暗号化の際に生成された乱数を取得する乱数取得手段をさらに含み、前記並替手段は暗号鍵の情報にこの乱数変数を加味してブロックを並べ替えるものである。

【００１８】

【発明の実施の形態】本発明の好適な実施の形態を適宜図面を参照して説明する。

【００１９】実施の形態１．実施の形態１に係る暗号化補助装置の特徴は、暗号化処理前に平文をブロック化し、そのブロックを秘密鍵データを用いて並べ替える点にある。秘密鍵データは暗号化側と復号化側の両者で共有する鍵である。

【００２０】図１は実施の形態１の暗号化補助装置１００の構成図である。同図のごとくこの装置は、暗号化すべき平文列を入力する入力部１と、入力された平文列を所定長のブロックに分割する分割部２と、秘密鍵の情報をもとにブロックを並べ替える並替部３と、並替後のブロックを先頭から順に図示しない暗号化装置に出力する出力部４とを有する。並替部３はさらに、秘密鍵をもとに各ブロックのシフト数を生成するシフト数生成部３ａと、そのシフト数に従って各ブロックの位置を実際に入れ替えるブロックシフト部３ｂを含む。このため、秘密鍵が並替部３に入力されている。なお、以上の各部は、例えばソフトウエアモジュールの形で存在し、これら各モジュールがメモリにロードされた形で、本装置が例えばパーソナルコンピュータによって実現される。これらのモジュールは、タンパフリー、つまり内部のアルゴリズムその他の情報を不正に見ようとした場合、機構的、電気的な破壊によって情報の読み出しが禁止される既知の構造のＩＣカードなどに一括して格納し、正当なユーザに配布することができる。この配布方法は以下すべての暗号化、復号化補助装置に適用できる。

【００２１】以上の構成において、まず処理の対象である平文が入力部１から入力される。この平文は分割部２で所定長、例えば６４ビットごとのブロックに分割され、並替部３に渡される。例えば秘密鍵が１２８ビットであり、入力された平文のブロック数がｎであってこれをＭ＝（Ｍ０，Ｍ１，…，Ｍｎ－１）と表す場合、並替

5

部３では以下の処理を行う。

【００２２】まずシフト数生成部３ａにおいて、秘密鍵のデータを８ビットずつに区分し、合計１６個の数Ｓ＝（Ｓ０，Ｓ１，…，Ｓ１５）を生成する。これが各ブロックのシフト数に相当するものであり、このＳがブロックシフト部３ｂに渡される。

【００２３】ブロックシフト部３ｂでは、Ｍｋを右側にＳｋだけシフトする。図２はこの様子を示しており、ここでは簡単な例で、

Ｓ＝（Ｓ０，Ｓ１，…，Ｓ１５）＝（３，１，２，０…）

としている。ＳとＭの添え字の一致に注目すれば、まずＭ０がＳ０＝３だけ右へシフトされ、つぎにＭ１がＳ１＝１だけ右へシフトされ、Ｍ２がＳ２＝２だけ右へシフトされる。以降、同様の処理をすべてのＭｋについて行い、並替部３によるブロックの並替が終了する。ここでは最終的にＭ’＝（Ｍ１，Ｍ３，Ｍ２，Ｍ０，Ｍ４，…，Ｍｎ－１）が得られる。なお、Ｓｋは８ビットであるから、Ｓｋの表す数値はしばしばブロック数ｎを超える。その場合も考慮するなら、Ｍｋのシフト数を剰余系を用いた（Ｓｋ　ｍｏｄ　ｎ）で計算すればよい。一方、ｎが１６を超える場合もありうるため、Ｍｋ（ｋ＞１５）については、そのシフト数をｉ＝（ｋ　ｍｏｄ　１６）なるＳｉをもとに決める。以上を定式化すれば、Ｍｋのシフト数は一般に、

Ｓｉ　ｍｏｄ　ｎ

ただし、ｉ＝（ｋ　ｍｏｄ　１６）

と記述できる。

【００２４】こうして並び替えられたブロックは、出力部４に送られる。出力部４は並替後のブロックの順に各ブロックを図示しない暗号化装置に出力し、そこで暗号化が行われる。以上が暗号化補助装置１００の動作である。　　一方、図３は実施の形態１に係る復号化補助装置１０１の構成図である。この装置は暗号化補助装置１００と逆の作用をなすものであり、復号化の後処理に利用される。すなわち、図１の暗号化補助装置１００を用いて暗号化された暗号文は、通常に復号化したとき、一見平文に戻ったように見えても、並替によってブロックの順序が正しくない（このような平文を以降「中間平文」とよぶ）。復号化補助装置１０１は中間平文を当初の平文に戻すよう働く。

【００２５】図３においてこの装置は、復号化装置で復号化された中間平文を入力する入力部８と、上述の暗号化補助装置１００の並替部３による並替をもとに戻す並替部９と、並替後のブロックを先頭から順に出力する出力部１０とを含む。並替部９はさらに、シフト数生成部９ａ、ブロックシフト部９ｂを含む。並替部９に秘密鍵が入力されている。中間平文は復号化の段階でブロックに分割されているため、本装置は分割部をもたない。出力部１０の出力先は、例えば表示装置など、最終的に得られた平文を必要とする任意の装置である。

6

【００２６】この構成において、まず暗号文は図示しない復号化装置で復号され、その結果得られた中間平文が入力部８から本装置に入力される。この中間平文は並替部９に送られる。シフト数生成部９ａは、暗号化補助装置１００のシフト数生成部３ａと全く同様に動作し、Ｓをブロックシフト部９ｂに与える。ブロックシフト部９ｂは二段階に動作する。前半の動作は暗号化補助装置１００のブロックシフト部３ｂと同じであり、図２のごとく、当初のＭ＝（Ｍ０，Ｍ１，…，Ｍｎ－１）からＭ’＝（Ｍ１，Ｍ３，Ｍ２，Ｍ０，Ｍ４，…，Ｍｎ－１）を得る。後半の動作は、Ｍ’とを照合することにより、各ブロックをもとの正しい位置に戻す。この例の場合、Ｍ’の第一ブロックはＭ１であるから、これを二番目のブロック位置に移動する。Ｍ’の第二ブロックはＭ３であるから、これを四番目のブロック位置に移動する。以下、同様にしてＭ’からＭを再生する。

【００２７】並替部９でもとの平文が得られた後、これは出力部１０に渡される。出力部１０はこの平文を必要とする任意の装置にこれを出力する。

【００２８】以上、実施の形態１によれば、従来の課題である第一ブロックの暗号強度を高めることができる。また、ブロックの並替を、暗号化および復号化の際に当然存在すべき暗号鍵を用いるため、新たな鍵を用意する必要もない。

【００２９】なお、実施の形態１の暗号化補助装置は、暗号化装置における暗号化方式は問わない。しかし、仮にＣＢＣ方式で暗号化される場合、この実施の形態のごとく並替を暗号化の後ではなく前に行うことに有用性がある。仮に並替を暗号化の後に行うとすれば、もとの第一ブロックが最初に暗号化されるため、このブロックに対するＣＢＣ方式のフィードバック効果がない。その状態で並替を行っても、第一ブロックについては、その位置は変わるが、暗号化の内容にランダム性を付加することはできない。したがって、特に第一ブロックが定型文の場合、実施の形態１のように並替を先に行ったほうが暗号強度が高まる。

【００３０】実施の形態２．実施の形態１では、ブロックの並替に秘密鍵データを用いた。実施の形態２では、秘密鍵データと暗号化補助装置内の時間変数を組み合わせて並替に用いる。このため、同じ秘密鍵を使用していても、この時間変数によって絶えず異なった並替が実現する。

【００３１】図４は実施の形態２の暗号化補助装置１０２の構成図である。同図において図１と同等の構成には同一の符号を与え、適宜説明を省略する。図４の特徴は、所定の基準タイミングに関して時間変数を生成する時間変数生成部１１と、そこで生成された時間変数を秘密鍵と同じビット数（ここでは１２８ビットとする）に拡張または短縮するハッシュ関数部１２が追加されてい

る点にある。「所定の基準タイミング」とは、一連の暗号化処理の中の特定のタイミングであり、例えば平文が入力部１に入力された瞬間などでよい。時間変数生成部１１は、例えばリアルタイムクロック、ソフトウエアタイマーなど、時間または時刻に関する情報を生成できる任意の構成でよい。ここでは一例として、時間変数がｈ：ｍ：ｓ（時間、分、秒）の６桁であるとする。ハッシュ関数部１２で１２８ビットにされた時間変数は、シフト数生成部１３ａとブロックシフト部１３ｂをもつ並替部１３に与えられる。ハッシュ関数には、例えばＭＤ５と呼ばれる既知の関数を採用すればよい。

【００３２】以上の構成による動作を実施の形態１との差異を中心に説明する。まず平文が入力部１から入力され、分割部２で分割される。分割の結果の複数のブロックは並替部１３に入力される。一方、時間変数生成部１１は、入力部１に平文が入力された瞬間の時刻ｈ：ｍ：ｓを時間変数としてハッシュ関数部１２に出力する。ハッシュ関数部１２は与えられた時間変数を１２８ビットに拡張してこれを並替部１３に渡す（以降、１２８ビットにされた時間変数を「拡張時間変数」とよぶ）。並替部１３のシフト数生成部１３ａは、数学的に可逆な方法、例えば排他的論理和をとる方法によって秘密鍵と拡張時間変数を合成し、合成後の１２８ビットのデータを実施の形態１同様１６個の数値Ｓ＝（Ｓ０，Ｓ１，…，Ｓ１５）に区分する。以下、ブロックシフト部１３ｂがこのＳを用いてブロックの並替を行う処理以降は実施の形態１同様である。ただし、実施の形態２では、最終的に作成された暗号文に対してもとの時間変数ｈ：ｍ：ｓを付加したうえで復号化補助装置に送るものとする。

【００３３】一方、図５は実施の形態２の復号化補助装置１０３の構成を示す。同図において図３との相違は、暗号化補助装置１０２から送られた時間変数を受け取る時間変数取得部１４と、その時間変数から拡張時間変数を生成するハッシュ関数部１５の追加である。ハッシュ関数は暗号化補助装置１０２と同一のものを用いる。

【００３４】この構成において、中間平文のブロックが実施の形態１同様、並替部１６に送られる。時間変数は、ハッシュ関数部１５により、暗号化補助装置１０２側と全く同じ拡張時間変数になる。並替部１６のシフト数生成部１６ａは秘密鍵と拡張時間変数を暗号化補助装置１０２側と同じ方法で合成し、数値の列Ｓを再現する。以下、ブロックの順序をもとに戻す手順は実施の形態１同様である。

【００３５】以上が実施の形態２の構成と動作である。実施の形態２によれば、ランダム性の高い時間情報を加味してブロックの並替ができるため、同じ暗号鍵を用いても、ほぼ毎回異なる並替ができる。したがって当然暗号強度も増す。

【００３６】なお、実施の形態２については次のような変形例が考えられる。第一の変形例として、ハッシュ関数部１５を削除し、単にもとの６桁の時間変数を秘密鍵の例えば上位６ビットに合成する。この方法によれば、構成が減る点にメリットがある。第二の変形例として、時間変数の代わりに拡張時間変数を復号化補助装置１０３に送付する方法がある。この方法によれば、復号化補助装置１０３の側にハッシュ関数部を設ける必要がない。

【００３７】実施の形態３．実施の形態２では、秘密鍵データに対して時間変数を加味してブロックの並替を行った。実施の形態３では、時間変数の代わりにユーザを識別するＩＤを利用する。

【００３８】図６は実施の形態３の暗号化補助装置１０４の構成を示す。同図と図４の違いは、時間変数生成部１１の代わりに外部からユーザのＩＤ情報を入力するためのＩＤ入力部１７が設けられる点にある。以下、ハッシュ関数部１８、並替部１９の動作は実施の形態２のものと同等である。実施の形態３では、最終的に作成された暗号文に対して、時間変数ではなくＩＤ情報を付加して復号化補助装置に送る。これはメッセージ等の送信に一般的な態様であり、実施の形態３の実現のうえで好都合である。

【００３９】一方、図７は実施の形態３の復号化補助装置１０５の構成を示す。同図と図５の違いは、時間変数取得部１４の代わりに、送付されてきたＩＤ情報を取得するためのＩＤ取得部２０が設けられる点にある。ここでもハッシュ関数部２１、並替部２２の動作は実施の形態２のものと同等である。なお、実施の形態３についても実施の形態２同様の変形例が考えられる。

【００４０】実施の形態４．実施の形態２では、秘密鍵データに対して時間変数を加味してブロックの並替を行った。実施の形態４では、時間変数の代わりに乱数を利用する。

【００４１】図８は実施の形態４の暗号化補助装置１０６の構成を示す。同図と図４の違いは、時間変数生成部１１の代わりに乱数を発生する乱数生成部２３が設けられる点にある。以下、ハッシュ関数部２４、並替部２５の動作は実施の形態２のものと同等である。実施の形態４では、最終的に作成された暗号文に対して、ブロックの並替に利用した乱数自体を付加して復号化補助装置に送る。

【００４２】一方、図９は実施の形態４の復号化補助装置１０７の構成を示す。同図と図５の違いは、時間変数取得部１４の代わりに、送付されてきた乱数情報を取得するための乱数取得部２６が設けられる点にある。ここでもハッシュ関数部２７、並替部２８の動作は実施の形態２のものと同等である。

【００４３】以上、実施の形態４によれば、暗号鍵の情報に乱数によるランダム性を付加することができるため、当然暗号強度が増す。

【００４４】

【発明の効果】本発明の暗号化補助方法では、暗号化に用いる暗号鍵の情報をもとに平文のブロックが並べ替えられるため、ブロックの位置に依存する暗号強度の低下を回避することができる。

【００４５】本発明の復号化補助方法では、復号化に用いた暗号鍵の情報をもとにその平文列を構成するブロックが並べ替えられるため、暗号化の際にブロックの並替があっても暗号文を正しくもとの平文に戻すことができる。このため、前記暗号化補助方法と併用することで、ブロックの位置に依存する暗号強度の低下を回避することができる。

【００４６】暗号鍵の情報をもとに分割されたブロックを並べ替える本発明の暗号化補助装置によれば、ブロックの位置に依存する暗号強度の低下を回避することができる。

【００４７】同様に、暗号鍵の情報をもとに入力された平文列を構成する各ブロックを並べ替える本発明の復号化補助装置によれば、暗号化の際にブロックの並替があっても暗号文を正しくもとの平文に戻すことができる。このため、前記暗号化補助装置と併用することで、ブロックの位置に依存する暗号強度の低下を回避することができる。

【００４８】時間変数を加味してブロックを並べ替える暗号化補助装置によれば、暗号鍵に対してランダム性を付加することができるため、暗号強度が高まる。

【００４９】同様に、時間変数を加味してブロックを並べ替える復号化補助装置によれば、暗号強度が高い状態が維持された状態で暗号文を受け取り、これをもとの平文に戻すことができる。

【００５０】ユーザーのＩＤ情報を加味してブロックを並べ替える暗号化補助装置によれば、ユーザーが通常何等かの形で入力すると考えられるＩＤ情報を用いるため、実現に都合がよい。また、ＩＤ情報の付加によって暗号強度も当然高まる。

【００５１】同様に、ＩＤ情報を加味してブロックを並べ替える復号化補助装置によれば、暗号強度が高い状態が維持された状態で暗号文を受け取り、これをもとの平文に戻すことができる。

【００５２】乱数を加味してブロックを並べ替える暗号

化補助装置によれば、ランダム性が高まるため、暗号強度を高めることができる。

【００５３】同様に、乱数を加味してブロックを並べ替える復号化補助装置によれば、暗号強度が高い状態が維持された状態で暗号文を受け取り、これをもとの平文に戻すことができる。

【図面の簡単な説明】

【図１】　実施の形態１の暗号化補助装置の構成図である。

【図２】　実施の形態１の暗号化補助装置の並替部の動作を示す図である。

【図３】　実施の形態１の復号化補助装置の構成図である。

【図４】　実施の形態２の暗号化補助装置の構成図である。

【図５】　実施の形態２の復号化補助装置の構成図である。

【図６】　実施の形態３の暗号化補助装置の構成図である。

【図７】　実施の形態３の復号化補助装置の構成図である。

【図８】　実施の形態４の暗号化補助装置の構成図である。

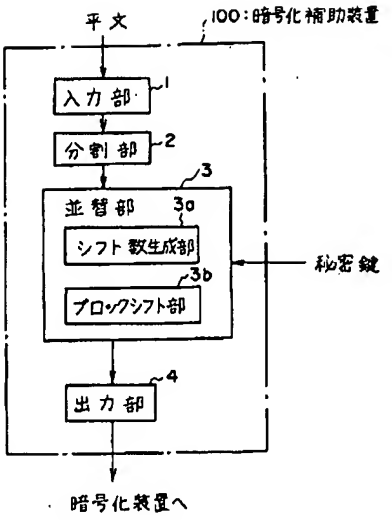
【図９】　実施の形態４の復号化補助装置の構成図である。

【図１０】　従来のブロック単位暗号化装置の構成図である。

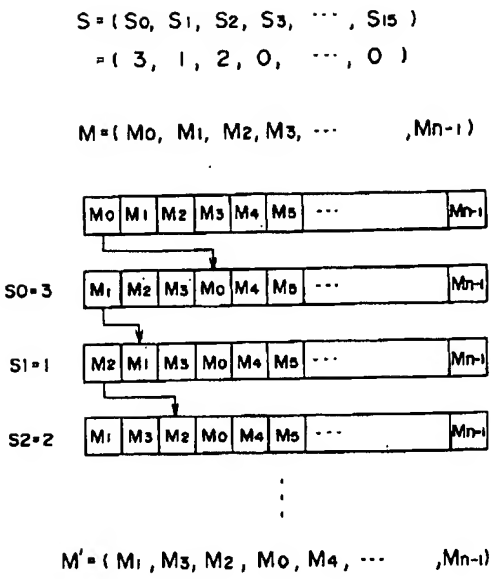
【符号の説明】

１，８　入力部、２　分割部、３，９，１３，１６，１９，２２，２５，２８並替部、３ａ，９ａ，１３ａ，１６ａ，１９ａ，２２ａ，２５ａ，２８ａ　シフト数生成部、３ｂ，９ｂ，１３ｂ，１６ｂ，１９ｂ，２２ｂ，２５ｂ，２８ｂブロックシフト部、４，１０　出力部、１１　時間変数生成部、１２，１５，１８，２１，２４，２７　ハッシュ関数部、１４　時間変数取得部、１７　ＩＤ入力部、２０　ＩＤ取得部、２３　乱数生成部、２６　乱数取得部、１００，１０２，１０４，１０６　暗号化補助装置、１０１，１０３，１０５，１０７　復号化補助装置。

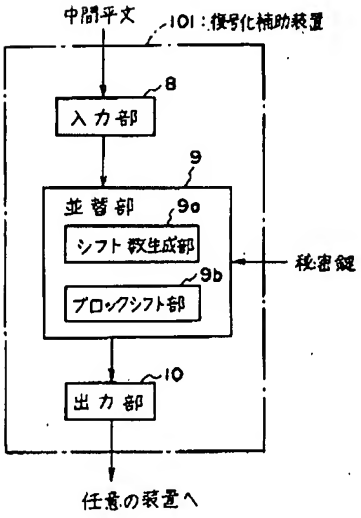
【図１】


平文
100:暗号化補助装置
入力部
1
分割部
2
3
並替部
3a
シフト数生成部
3b
ブロックシフト部
秘密鍵
4
出力部
暗号化装置へ

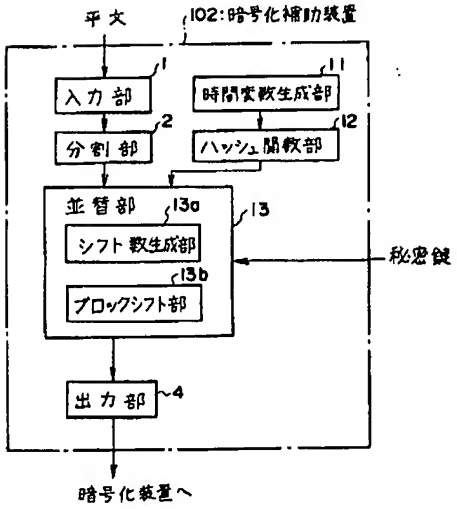
【図２】


S=(So, S1, S2, S3, ···, S15)
=(3, 1, 2, 0, ···, 0)
M=(Mo, M1, M2, M3, ···, Mn-1)
Mo M1 M2 M3 M4 M5 ··· Mn-1
S0=3
M1 M2 M3 Mo M4 M5 ··· Mn-1
S1=1
M2 M1 M3 Mo M4 M5 ··· Mn-1
S2=2
M1 M3 M2 Mo M4 M5 ··· Mn-1
M'=(M1, M3, M2, Mo, M4, ···, Mn-1)

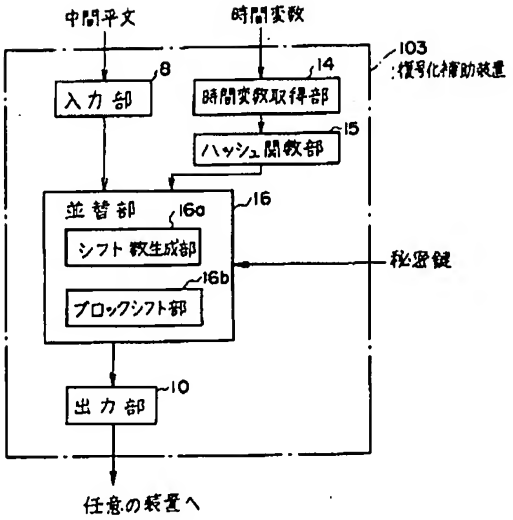
【図３】


中間平文
101:復号化補助装置
8
入力部
9
並替部
9a
シフト数生成部
9b
ブロックシフト部
秘密鍵
10
出力部
任意の装置へ

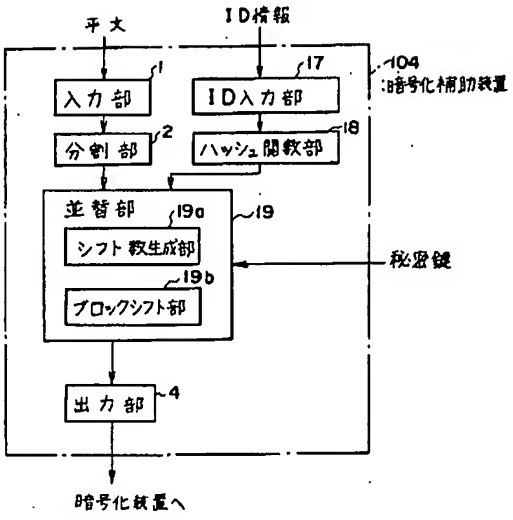
【図４】


平文
102:暗号化補助装置
1
入力部
11
時間変数生成部
2
分割部
12
ハッシュ関数部
並替部
13a
13
シフト数生成部
13b
ブロックシフト部
秘密鍵
4
出力部
暗号化装置へ

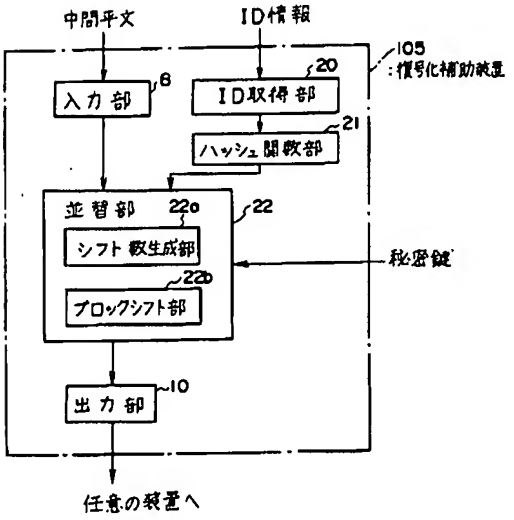
【図５】


中間平文
時間変数
103
:暗号化補助装置
入力部
8
時間変数取得部
14
ハッシュ関数部
15
並替部
16
16a
シフト数生成部
16b
ブロックシフト部
秘密鍵
出力部
10
任意の装置へ

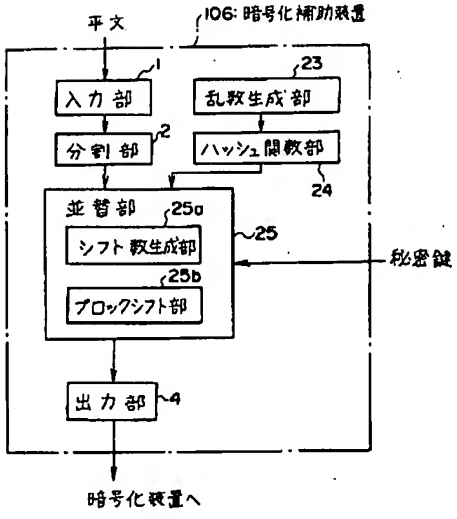
【図６】


平文
ID情報
104
:暗号化補助装置
入力部
1
ID入力部
17
分割部
2
ハッシュ関数部
18
並替部
19
19a
シフト数生成部
19b
ブロックシフト部
秘密鍵
出力部
4
暗号化装置へ

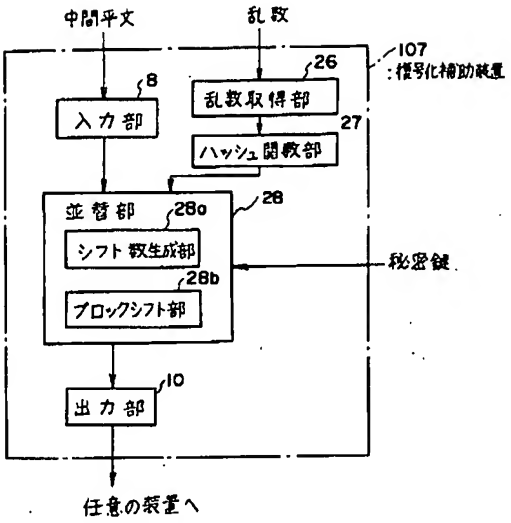
【図７】


中間平文
ID情報
105
:暗号化補助装置
入力部
8
ID取得部
20
ハッシュ関数部
21
並替部
22
22a
シフト数生成部
22b
ブロックシフト部
秘密鍵
出力部
10
任意の装置へ

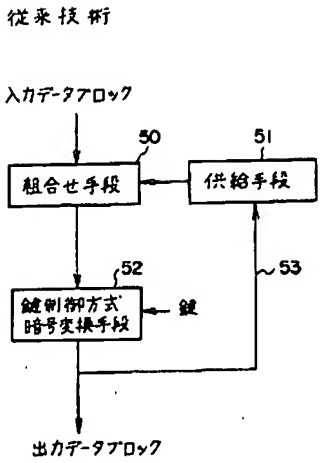
【図８】


平文
106: 暗号化補助装置
入力部
1
乱数生成部
23
分割部
2
ハッシュ関数部
24
並替部
25
25a
シフト数生成部
25b
ブロックシフト部
秘密鍵
出力部
4
暗号化装置へ

【図９】


中間平文
乱数
107
：暗号化補助装置
8
入力部
26
乱数取得部
27
ハッシュ関数部
並替部
28a
シフト数生成部
28
28b
ブロックシフト部
秘密鍵
10
出力部
任意の装置へ

【図１０】


従来技術
入力データブロック
50
51
組合せ手段
供給手段
52
53
鍵制御方式
暗号変換手段
鍵
出力データブロック

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-173646

(43)Date of publication of application : 26.06.1998

(51)Int.Cl. H04L 9/34
G09C 1/00
G09C 1/00
H04L 9/14

(21)Application number : 08-334023

(22)Date of filing : 13.12.1996

(71)Applicant : MITSUBISHI ELECTRIC CORP

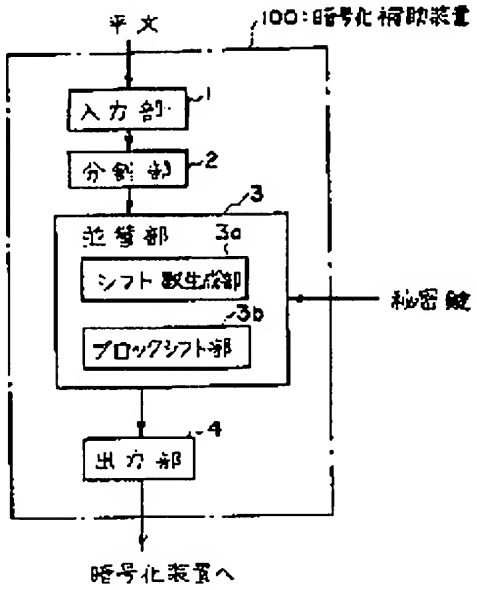
(72)Inventor : HASEGAWA TOSHIO

(54) CIPHERING ASSISTING METHOD, DECODING ASSISTING METHOD AND DEVICE USING THEM

(57)Abstract:

PROBLEM TO BE SOLVED: To inhibit the deterioration of cryptographic intensity, due to the position of a block such as a first block.

SOLUTION: This ciphering assisting device is provided with an input part 1 for inputting a regular sentence string to be ciphered, a division part 2 for dividing the inputted regular sentence string into the blocks of prescribed length, a rearranging part 3 for rearranging the divided blocks, based on information of the password key and an output part 4 for outputting the blocks, after rearrangement to the ciphering device of a post stage in order from the head has been made. When data of the secret key is '3, 1, 2...', for example, the first block is shifted to the right by three, than the second block is shifted to the right by one, and the third block is shifted to the right by two and the order blocks is exchanged.



LEGAL STATUS

[Date of request for examination] 28.07.2003

[Date of sending the examiner's decision of rejection] 25.04.2006

[Kind of final disposal of application other than the examiner's decision of rejection or

* NOTICES *

JPO and INPIT are not responsible for any damages caused by the use of this translation.

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]
[Claim 1] The encryption auxiliary approach characterized by dividing into the block of predetermined length the plaintext train which should be enciphered, rearranging a block based on the information on the cryptographic key used for encryption, and handing over the block after a sort to encryption down stream processing sequentially from a head.
[Claim 2] The decryption auxiliary approach characterized by rearranging the block which constitutes the plaintext train based on the information on the cryptographic key which used for reception and a decryption the plaintext train decrypted by decryption down stream processing, and outputting the block after a sort sequentially from a head.
[Claim 3] The encryption auxiliary device carry out having an input means input the plaintext train which is equipment which performs auxiliary processing on the occasion of encryption of the plaintext using a cryptographic key, and should encipher, a division means divide the inputted plaintext train into the block of predetermined length, the sort means that rearrange the divided block based on the information on a cryptographic key, and an output means output the block after a sort to the encryption processing section sequentially from a head as the description.
[Claim 4] The decryption auxiliary device characterized by to have the sort means which rearranges each block which is equipment which performs auxiliary processing on the occasion of a decryption of the cipher using a cryptographic key, and constitutes the plaintext train inputted based on the information on a cryptographic key as an input means input the plaintext train decrypted in the decryption processing section, and an output means output the block after a sort sequentially from a head.
[Claim 5] Said sort means is an encryption auxiliary device according to claim 3 which seasons the information on a cryptographic key with this time amount variable, and rearranges a block, including further a time amount variable generation means to generate a time amount variable about predetermined criteria timing.
[Claim 6] Said sort means is a decryption auxiliary device according to claim 4 which seasons the information on a cryptographic key with this time amount variable, and rearranges a block, including further a time amount variable acquisition means to acquire the time amount variable generated about the criteria timing in the case of encryption.
[Claim 7] Said sort means is an encryption auxiliary device according to claim 3 which seasons the information on a cryptographic key with this ID information, and rearranges a block, including further an ID input means to input ID information which identifies a user.
[Claim 8] Said sort means is a decryption auxiliary device according to claim 4 which seasons the information on a cryptographic key with this time amount variable, and rearranges a block, including further an ID acquisition means to acquire ID information inputted on the occasion of encryption.
[Claim 9] Said sort means is an encryption auxiliary device according to claim 3 which seasons the information on a cryptographic key with this random-number information, and rearranges a block, including further a random-number generation means to generate a random number.
[Claim 10] Said sort means is a decryption auxiliary device according to claim 4 which seasons the information on a cryptographic key with this random-number variable, and rearranges a block, including further a random-number acquisition means to acquire the random number generated on the occasion of encryption.

[Translation done.]

* NOTICES *

JPO and INPIT are not responsible for any damages caused by the use of this translation.

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention] This invention relates to the approach and equipment which perform auxiliary processing on the occasion of encryption and a decryption.
[0002]
[Description of the Prior Art] The public key cryptosystem RSA (Rivest-Shamir-Adlemen) which pays its attention to the private key cryptosystem DES (Data Encryption Standard) which is a U.S. standard code, and factorization in prime numbers as a conventional cipher system is known. In these cipher systems, it is characterized by finally enciphering the whole plaintext by enciphering a plaintext with a public key or a private key per a break and block to a certain fixed block. Although the code reinforcement of these methods, i.e., decode, is carried out and hard is very high, since it processes per block, it can become the cause by which a fixed statistical property may be shown for every block, and this reduces code reinforcement according to the class of plaintext etc.
[0003] In order to raise the encryption reinforcement of the block base, a method called cipher block chaining is learned. For example, ISO8372 has prescribed four kinds of code modes CBC, OFB, and CFB, and ECB mode. A code machine is made to recur the information based on [whenever it enciphers one plaintext block] the result or progress, and the information is made to influence the encryption after degree block continuously in these modes (except for ECB). According to these modes, decode becomes difficult in order that encryption of a certain block may be dependent on the hysteresis of the past encryption processing.
[0004] As encryption equipment of such the conventional block base, the notional configuration of the equipment indicated by drawing 10 at JP,52-130505,U is shown. In this drawing, a combination means which combines an reversible function and an input data block mathematically to be dependent on the data word whose 50 is a former output data block, a supply means by which 51 supplies data word to a combination means, and 52 are key control-system code conversion means which encipher based on a user's key.
[0005] If an input data block is inputted with this configuration, the data word 53 which had already existed in the key control-system code conversion means 52 then will be outputted to the combination means 50 by the supply means 51. The combination means 50 combines the reversible function decided by data word 53, and a new input data block, and the result is passed to the key control-system code conversion means 52. The key control-system code conversion means 52 enciphers a data block with the application of the function of a key, and outputs this. This output is passed to the supply means 51 as new data word 53.
[0006]
[Problem(s) to be Solved by the Invention] In cipher block chaining (CBC, OFB, CFB mode, etc.), since the complicated encryption function which wove in the past code hysteresis is used, generally decode becomes difficult. However, since the block preceded with the block does not exist in case the first block of a plaintext is enciphered, the effectiveness by the chain is not acquired. For example, when assuming an electronic mail, that beginning of a sentence is a fixed form in many cases, and the plaintext data of a basis are easy to be expected about this part. Even if the contents of the electronic mail differ, since it is processed with the encryption function same each time, the first block of the key of decode may be given to the inside which continues use of the same CBC method.
[0007] This invention is made in view of such a technical problem, and the purpose is in offering the

encryption auxiliary approach and equipment which prevent the fall of the code reinforcement resulting from the location of blocks, such as the first block. Another purpose of this invention is to offer the decryption auxiliary approach and equipment which can return the cipher enciphered with those approaches or equipment to a plaintext.

[0008]

[Means for Solving the Problem] The encryption auxiliary approach of this invention divides into the block of predetermined length the plaintext train which should be enciphered, rearranges a block based on the information on the cryptographic key used for encryption, and hands over the block after a sort to encryption down stream processing sequentially from a head.

[0009] On the other hand, the decryption auxiliary approach of this invention rearranges the block which constitutes the plaintext train based on the information on the cryptographic key which used for reception and a decryption the plaintext train decrypted from decryption down stream processing, and outputs the block after a sort sequentially from a head.

[0010] On the other hand, the encryption auxiliary device of this invention has an input means to input the plaintext train which should be enciphered, a division means to divide the inputted plaintext train into the block of predetermined length, the sort means that rearranges the divided block based on the information on a cryptographic key, and an output means output the block after a sort to the encryption processing section sequentially from a head.

[0011] Moreover, the decryption auxiliary device of this invention has the sort means which rearranges each block which constitutes the plaintext train inputted as an input means to input the plaintext train decrypted in the decryption processing section, based on the information on a cryptographic key, and an output means to output the block after a sort sequentially from a head.

[0012] Including further a time amount variable generation means by which the encryption auxiliary device of this invention generates a time amount variable about predetermined criteria timing, said sort means seasons the information on a cryptographic key with this time amount variable, and rearranges a block.

[0013] Including further a time amount variable acquisition means to acquire the time amount variable with which the decryption auxiliary device of this invention was generated about the criteria timing in the case of encryption, said sort means seasons the information on a cryptographic key with this time amount variable, and rearranges a block.

[0014] Including further an ID input means by which the encryption auxiliary device of this invention inputs ID information which identifies a user, said sort means seasons the information on a cryptographic key with this ID information, and rearranges a block.

[0015] Including further an ID acquisition means to acquire ID information as which the decryption auxiliary device of this invention was inputted on the occasion of encryption, said sort means seasons the information on a cryptographic key with this time amount variable, and rearranges a block.

[0016] Including further a random-number generation means by which the encryption auxiliary device of this invention generates a random number, said sort means seasons the information on a cryptographic key with this random-number information, and rearranges a block.

[0017] Including further a random-number acquisition means to acquire the random number with which the decryption auxiliary device of this invention was generated on the occasion of encryption, said sort means seasons the information on a cryptographic key with this random-number variable, and rearranges a block.

[0018]

[Embodiment of the Invention] The gestalt of suitable operation of this invention is suitably explained with reference to a drawing.

[0019] The description of the encryption auxiliary device concerning the gestalt 1 of gestalt 1. implementation of operation blocks a plaintext before encryption processing, and is that it rearranges the block using private key data. Private key data are a key shared between both by the side of encryption and a decryption.

[0020] Drawing 1 is the block diagram of the encryption auxiliary device 100 of the gestalt 1 of operation. As shown in this drawing, this equipment has the input section 1 which inputs the plaintext train which should be enciphered, the division section 2 which divides the inputted plaintext train into the block of predetermined length, the sort section 3 which rearranges a block based on the information on a private key, and the output section 4 which outputs the block after a sort to the encryption equipment which is not illustrated sequentially from a head. The sort section 3 contains block shift

section 3b which actually replaces the location of each block with shift count generation section 3a which generates the shift count of each block further according to the shift count based on a private key. For this reason, the private key is inputted into the sort section 3. In addition, the above each part exists in the form of a software module, it is the form where each [these] module was loaded to memory, and this equipment is realized by the personal computer. When it is going to see unjustly the Tampa free-lancer's, i.e., an internal algorithm and internal others, information, these modules can be collectively stored in the IC card of the known structure where read-out of information is forbidden etc., by structural and electric destruction, and can be distributed to a valid user. This distribution approach is below applicable to all encryption and decryption auxiliary devices.

[0021] In the above configuration, the plaintext which is the object of processing first is inputted from the input section 1. This plaintext is divided into the predetermined length in every 64 bits, for example, a block, in the division section 2, and is passed to the sort section 3. For example, a private key is 128 bits, the block count of the inputted plaintext is n, and when it expresses this as M= (M0, M1, --, Mn-1), the following processings are performed in the sort section 3.

[0022] First, in shift count generation section 3a, it classifies the data of a private key into 8 bits at a time, and several [a total of 16] S= (S0, S1, --, S15) is generated. This is equivalent to the shift count of each block, and this S is passed to block shift section 3b.

[0023] In block shift section 3b, only Sk shifts Mk to right-hand side. Drawing 2 shows this situation, is an easy example here, and is S=(S0, S1, --, S15) = (3, 1, 2, 0 --).

It is carrying out. If it takes notice of coincidence of the suffix of S and M, M0 is first shifted to the right only for S0= 3, next, M1 will be shifted to the right only for S1= 1, and M2 will be shifted to the right only for S2= 2. Henceforth, same processing is performed about all Mk(s) and the sort of the block by the sort section 3 is completed. Here, finally M'= (M1, M3, M2, M0, M4, --, Mn-1) is obtained. In addition, since Sk is 8 bits, the numeric value which Sk expresses often exceeds block count n. if it takes into consideration also in that case -- the shift count of Mk -- a system of residues -- having used (Sk mod n) -- what is necessary is just to calculate since n can exceed 16 on the other hand -- Mk (k> 15) -- the shift count -- i= (k mod 16) -- it decides based on Si. If the above is formulized, generally the shift count of Mk will be Si. mod n, however i= (k mod 16)

It can describe.

[0024] In this way, the rearranged block is sent to the output section 4. The output section 4 is outputted to the encryption equipment which does not illustrate each block in order of the block after a sort, and encryption is performed there. The above is actuation of the encryption auxiliary device 100. On the other hand, drawing 3 is the block diagram of the decryption auxiliary device 101 concerning the gestalt 1 of operation. This equipment makes an operation contrary to the encryption auxiliary device 100, and is used for the after treatment of a decryption. That is, when it decrypts to usual, even if the cipher enciphered using the encryption auxiliary device 100 of drawing 1 seems to have returned to the plaintext apparently, the sequence of a block by the sort is not right (such a plaintext is henceforth called a "middle plaintext"). The decryption auxiliary device 101 works so that a middle plaintext may be returned to the original plaintext.

[0025] In drawing 3 , this equipment contains the input section 8 which inputs the middle plaintext decrypted with decryption equipment, the sort section 9 which returns the sort by the sort section 3 of the above-mentioned encryption auxiliary device 100, and the output section 10 which outputs the block after a sort sequentially from a head. The sort section 9 contains shift count generation section 9a and block shift section 9b further. The private key is inputted into the sort section 9. Since the middle plaintext is divided into the block in the phase of a decryption, this equipment does not have the division section. The output destination changes of the output section 10 are equipments of arbitration which need the plaintext finally obtained, such as a display.

[0026] In this configuration, first, a cipher is decoded with the decryption equipment which is not illustrated and the middle plaintext obtained as a result is inputted into this equipment from the input section 8. This middle plaintext is sent to the sort section 9. Shift count generation section 9a operates completely like shift count generation section 3a of the encryption auxiliary device 100, and gives S to block shift section 9b. Block shift section 9b operates to two steps. Actuation of the first half is the same as block shift section 3b of the encryption auxiliary device 100, and obtains M= (M0, M1, --, Mn-1) to M'= (M1, M3, M2, M0, M4, --, Mn-1) of the beginning like drawing 2 . Actuation of the second half returns each block to the right location of a basis by collating M' and M. Since the first block of M' is M1 in the case of this example, this is moved to the second block location. Since the second block of M'

is M3, it moves this to the fourth block location. Hereafter, M is similarly reproduced from M'.
[0027] This is passed to the output section 10 after the plaintext of a basis is obtained in the sort section 9. The output section 10 outputs this to the equipment of arbitration which needs this plaintext.
[0028] As mentioned above, according to the gestalt 1 of operation, the code reinforcement of the first block which is the conventional technical problem can be raised. Moreover, in order to use the cryptographic key which should naturally exist the sort of a block in the case of encryption and a decryption, it is not necessary to prepare a new key.
[0029] In addition, the encryption auxiliary device of the gestalt 1 of operation does not ask the cipher system in encryption equipment. However, when temporarily enciphered by the CBC method, usefulness is like the gestalt of this operation to carry out to the front after enciphering a sort. If it carries out temporarily after enciphering a sort, since the first block of a basis is enciphered first, there is no feedback effect of the CBC method to this block. Even if it performs a sort in the condition, although the location changes, about the first block, it cannot add random nature to the contents of encryption. Therefore, when especially the first block is a fixed form sentence, code reinforcement increases [the way which performed the sort previously like the gestalt 1 of operation].
[0030] Private key data were used for the sort of a block with the gestalt 1 of gestalt 2. implementation of operation. With the gestalt 2 of operation, it uses for a sort combining the time amount variable in private key data and an encryption auxiliary device. For this reason, even if it is using the same private key, the sort which changed continuously with these time amount variables is realized.
[0031] Drawing 4 is the block diagram of the encryption auxiliary device 102 of the gestalt 2 of operation. The same sign is given to a configuration equivalent to drawing 1 in this drawing, and explanation is omitted suitably. The description of drawing 4 is in the point that the time amount variable generation section 11 which generates a time amount variable about predetermined criteria timing, and the Hash Function section 12 which extends or shortens the time amount variable generated there to the same number of bits (here, it may be 128 bits) as a private key are added. "Predetermined criteria timing" is the specific timing in a series of encryption processings, for example, it is good at the moment that a plaintext is inputted into the input section 1 etc. A real time clock, the software timer of the time amount variable generation section 11, etc. are good with the configuration of the arbitration which can generate time amount or the information about time of day. Here, suppose as an example that a time amount variable is 6 figures of h:m:second (time amount, a part, second). The time amount variable made into 128 bits in the Hash Function section 12 is given to the sort section 13 with shift count generation section 13a and block shift section 13b. What is necessary is just to adopt the known function called MD5 as a Hash Function.
[0032] It explains focusing on a difference with the gestalt 1 of operation of actuation by the above configuration. First, a plaintext is inputted from the input section 1 and divided in the division section 2. Two or more blocks as a result of division are inputted into the sort section 13. On the other hand, the time amount variable generation section 11 is outputted to the Hash Function section 12 by making into a time amount variable time-of-day h:m:second of the moment that a plaintext is inputted into the input section 1. The Hash Function section 12 extends the given time amount variable to 128 bits, and passes this to the sort section 13 (the time amount variable made into 128 bits is henceforth called an "extended time amount variable"). Mathematically, by the reversible approach, for example, the method of taking an exclusive OR, shift count generation section 13a of the sort section 13 compounds a private key and an extended time amount variable, and classifies the 128-bit data after composition into 16 numeric-values S= (S0, S1, --, S15) like the gestalt 1 of operation. It is the same as that of the gestalt 1 of operation after the processing whose block shift section 13b performs the sort of a block hereafter using this S. However, with the gestalt 2 of operation, after adding time amount variable h:m:second of a basis to the cipher finally created, it shall send to a decryption auxiliary device.
[0033] On the other hand, drawing 5 shows the configuration of the decryption auxiliary device 103 of the gestalt 2 of operation. In this drawing, the difference with drawing 3 is the addition of the time amount variable acquisition section 14 which receives the time amount variable sent from the encryption auxiliary device 102, and the Hash Function section 15 which generates an extended time amount variable from the time amount variable. A Hash Function uses the same thing as the encryption auxiliary device 102.
[0034] In this configuration, the block of a middle plaintext is sent to the sort section 16 like the gestalt 1 of operation. A time amount variable turns into the completely same extended time amount variable as the encryption auxiliary device 102 side by the Hash Function section 15. Shift count generation section

16a of the sort section 16 compounds a private key and an extended time amount variable by the same approach as the encryption auxiliary device 102 side, and reproduces the numerical train S. The procedure of returning the sequence of a block hereafter is the same as that of the gestalt 1 of operation.
[0035] The above is the configuration and actuation of the gestalt 2 of operation. Since according to the gestalt 2 of operation the high hour entry of random nature is considered and the sort of a block is made, even if it uses the same cryptographic key, a sort different almost each time is made. Therefore, naturally code reinforcement also increases.
[0036] In addition, the following modifications can be considered about the gestalt 2 of operation. As the first modification, the Hash Function section 15 is deleted and the time amount variable of 6 figures of a basis is only compounded on 6 bits of high orders of a private key. According to this approach, a merit is in the point whose configuration decreases. As the second modification, there is a method of sending an extended time amount variable to the decryption auxiliary device 103 instead of a time amount variable. According to this approach, it is not necessary to prepare the Hash Function section in the decryption auxiliary device 103 side.
[0037] With the gestalt 2 of gestalt 3. implementation of operation, the time amount variable was considered to private key data, and the sort of a block was performed. With the gestalt 3 of operation, ID which identifies a user instead of a time amount variable is used.
[0038] Drawing 6 shows the configuration of the encryption auxiliary device 104 of the gestalt 3 of operation. The difference between this drawing and drawing 4 is in the point that ID input section 17 for inputting a user's ID information from the exterior instead of the time amount variable generation section 11 is formed. Actuation of the following and Hash Function section 18 and the sort section 19 is equivalent to the thing of the gestalt 2 of operation. With the gestalt 3 of operation, to the cipher finally created, not a time amount variable but ID information is added, and it sends to a decryption auxiliary device. This is a mode general to transmission of a message etc., and after realizing the gestalt 3 of operation, it is convenient.
[0039] On the other hand, drawing 7 shows the configuration of the decryption auxiliary device 105 of the gestalt 3 of operation. The difference between this drawing and drawing 5 is in the point that ID acquisition section 20 for acquiring sent ID information instead of the time amount variable acquisition section 14 is formed. Actuation of the Hash Function section 21 and the sort section 22 is equivalent to the thing of the gestalt 2 of operation also here. In addition, the modification same also about the gestalt 3 of operation as the gestalt 2 of operation can be considered.
[0040] With the gestalt 2 of gestalt 4. implementation of operation, the time amount variable was considered to private key data, and the sort of a block was performed. With the gestalt 4 of operation, a random number is used instead of a time amount variable.
[0041] Drawing 8 shows the configuration of the encryption auxiliary device 106 of the gestalt 4 of operation. The difference between this drawing and drawing 4 is in the point that the random-number generation section 23 which generates a random number instead of the time amount variable generation section 11 is formed. Actuation of the following and Hash Function section 24 and the sort section 25 is equivalent to the thing of the gestalt 2 of operation. With the gestalt 4 of operation, the random number itself used for the sort of a block is added to the cipher finally created, and it sends to a decryption auxiliary device.
[0042] On the other hand, drawing 9 shows the configuration of the decryption auxiliary device 107 of the gestalt 4 of operation. The difference between this drawing and drawing 5 is in the point that the random-number acquisition section 26 for acquiring the sent random-number information instead of the time amount variable acquisition section 14 is formed. Actuation of the Hash Function section 27 and the sort section 28 is equivalent to the thing of the gestalt 2 of operation also here.
[0043] As mentioned above, according to the gestalt 4 of operation, since the random nature by the random number can be added to the information on a cryptographic key, naturally, code reinforcement increases.
[0044]
[Effect of the Invention] By the encryption auxiliary approach of this invention, since the block of a plaintext is rearranged based on the information on the cryptographic key used for encryption, the fall of code reinforcement depending on the location of a block is avoidable.
[0045] Since the block which constitutes the plaintext train from a decryption auxiliary approach of this invention based on the information on the cryptographic key used for the decryption is rearranged, in case it is encryption, even if there is a sort of a block, a cipher can be correctly returned to the plaintext

of a basis. For this reason, the fall of code reinforcement depending on the location of a block is avoidable by using together with said encryption auxiliary approach.

[0046] According to the encryption auxiliary device of this invention which rearranges the block divided based on the information on a cryptographic key, the fall of code reinforcement depending on the location of a block is avoidable.

[0047] According to the decryption auxiliary device of this invention which rearranges each block which similarly constitutes the plaintext train inputted based on the information on a cryptographic key, even if there is a sort of a block in the case of encryption, a cipher can be correctly returned to the plaintext of a basis. For this reason, the fall of code reinforcement depending on the location of a block is avoidable by using together with said encryption auxiliary device.

[0048] According to the encryption auxiliary device which considers a time amount variable and rearranges a block, since random nature can be added to a cryptographic key, code reinforcement increases.

[0049] According to the decryption auxiliary device which similarly considers a time amount variable and rearranges a block, where the condition that code reinforcement is high is maintained, a cipher can be returned to reception and this can be returned to the plaintext of a basis.

[0050] In order to use ID information considered that a user usually inputs in a certain form according to the encryption auxiliary device which considers a user's ID information and rearranges a block, it is convenient for implementation. Moreover, naturally code reinforcement also increases by addition of ID information.

[0051] According to the decryption auxiliary device which similarly considers ID information and rearranges a block, where the condition that code reinforcement is high is maintained, a cipher can be returned to reception and this can be returned to the plaintext of a basis.

[0052] According to the encryption auxiliary device which considers a random number and rearranges a block, since random nature increases, code reinforcement can be raised.

[0053] According to the decryption auxiliary device which similarly considers a random number and rearranges a block, where the condition that code reinforcement is high is maintained, a cipher can be returned to reception and this can be returned to the plaintext of a basis.

[Translation done.]

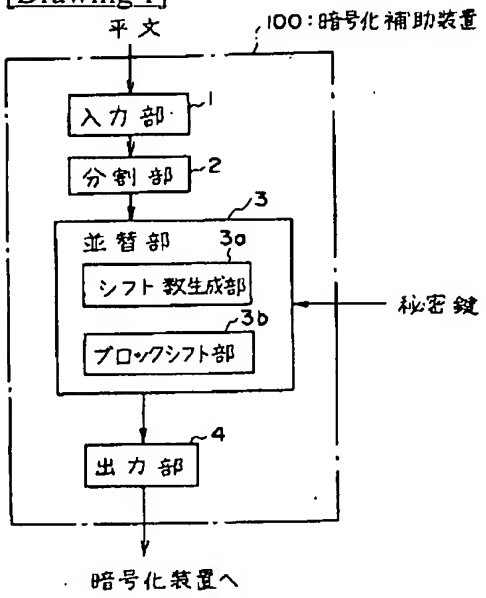
* NOTICES *

JPO and INPIT are not responsible for any damages caused by the use of this translation.

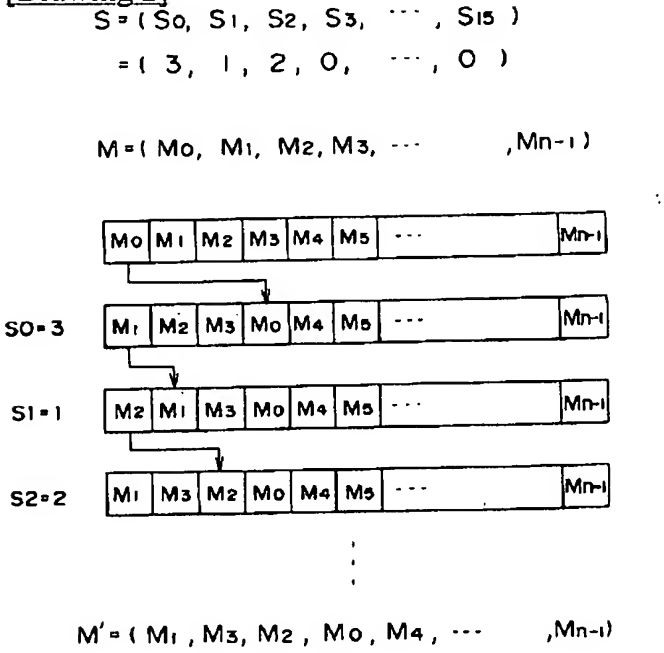
1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DRAWINGS

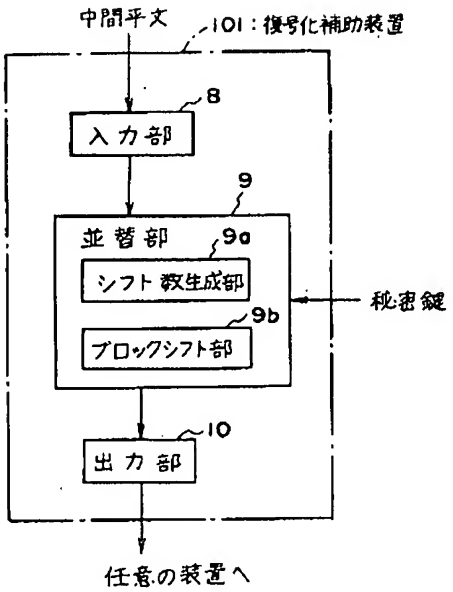
[Drawing 1]



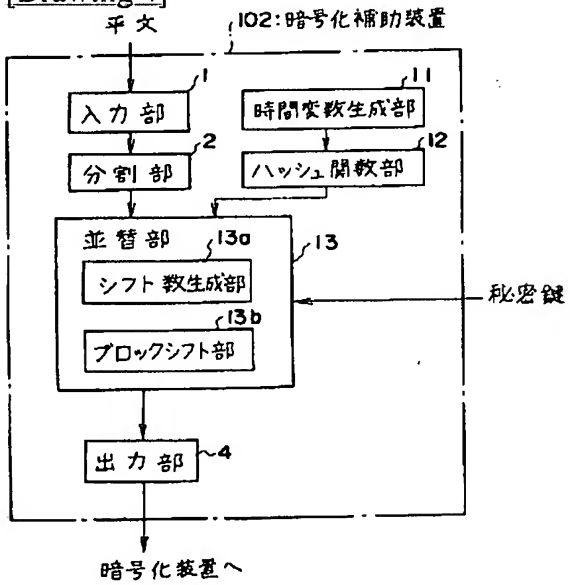
[Drawing 2]



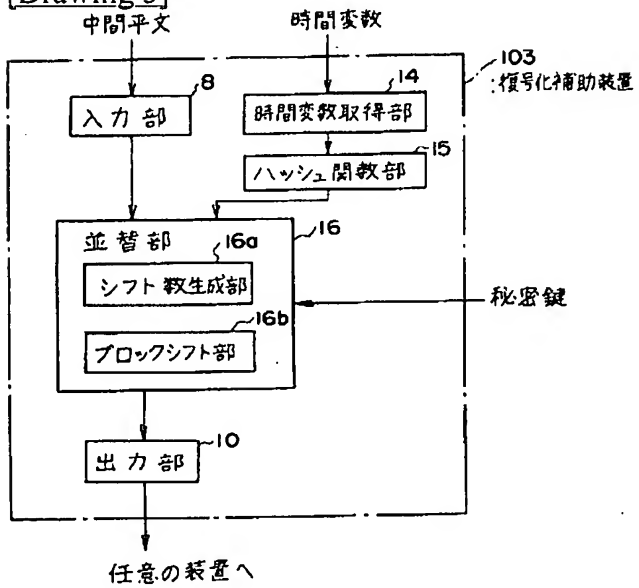
[Drawing 3]



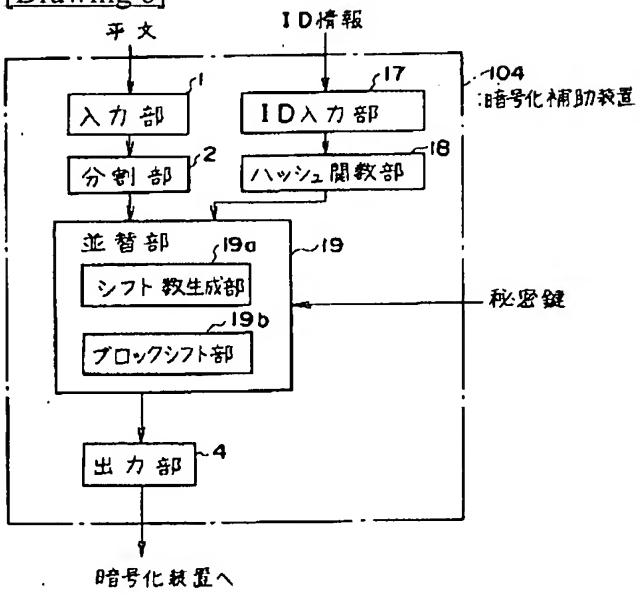
[Drawing 4]



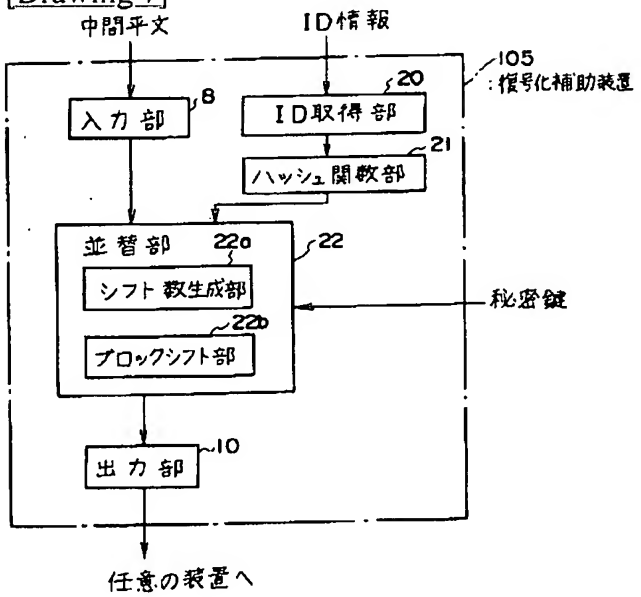
[Drawing 5]



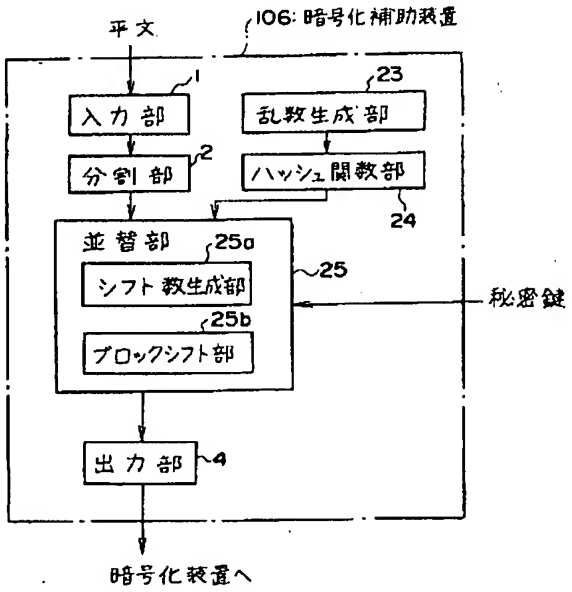
[Drawing 6]



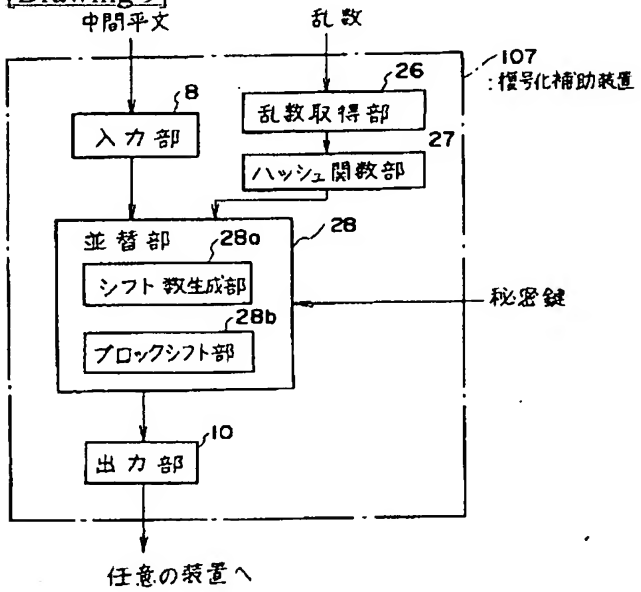
[Drawing 7]



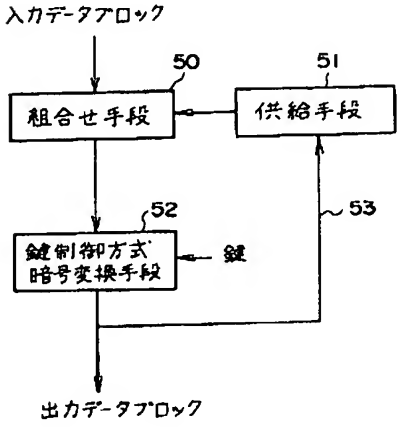
[Drawing 8]



[Drawing 9]



[Drawing 10]
従来技術



[Translation done.]